

## **EU-DSGVO kompakt für Kosmetikerinnen und Kosmetiker**

Die EU-DSGVO schafft es in diesem Jahr, wie keine andere Verordnung vorher für echte Verunsicherung zu sorgen.

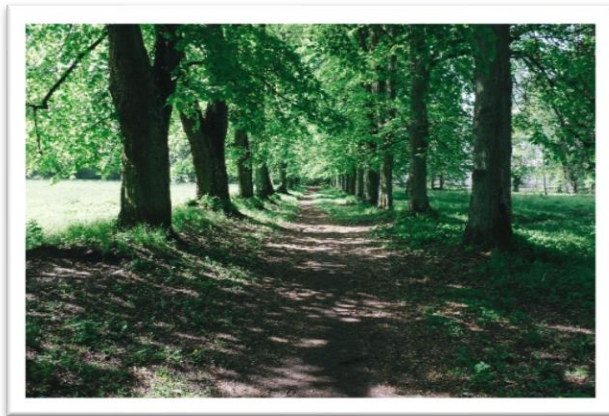
Sicherlich geht es euch auch so, dass ihr das Gefühl habt, überhaupt nicht durchzublicken. Seid ganz beruhigt, denn so geht es wirklich den Meisten gerade.

Es gibt einfach viel zu viele Informationen online. Dazu kommen Menschen, die Halbwahrheiten und Angst verbreiten - wie soll man da noch durchblicken?

Und sind wir mal ehrlich: Gesetze, Recht und Verordnungen - da ist einem doch der Zahnarztbesuch fast lieber 😊.

Drumherum zu reden hilft aber auch nicht, denn ab dem 25. Mai 2018 wird es aber soweit sein und die EU-Datenschutzgrundverordnung (DSGVO) tritt in Kraft.

Also erstmal: DURCHATMEN!



### **Wir gehen den Weg gemeinsam!**

Es ist vor allem wichtig, mit einer positiven Grundhaltung an das Thema heranzugehen, denn ändern können wir daran nichts mehr.

#### DISCLAIMER

Dieses Dokument dient einer allgemeinen Information und stellt KEINE Rechtsberatung im Einzelfall dar. Sämtliche Muster müssen auf den Einzelfall angepasst werden. Zudem wird keine Gewähr für Aktualität und Vollständigkeit übernommen. Die Vervielfältigung ist kostenlos unter Verwendung der Urheberkennzeichnung gestattet.

Ihr werdet sehen, dass es gar nicht so viele Dinge sind, an die wir künftig denken müssen.

Die erste Frage ist natürlich immer: „Was habe ich überhaupt mit der EU-DSGVO zu tun? Es trifft doch sicher nur große Unternehmen, oder?“

Leider muss ich euch an dieser Stelle die Augen öffnen, denn die EU-DSGVO trifft jeden, der in der EU personenbezogene Daten verarbeitet (Was das wiederum genau bedeutet, erkläre ich gleich noch!).

Selbst, wenn man schnell aus der EU wegziehen würde, nützt es nichts, da selbst dann, wenn man in einem sogenannten Nicht-EU-Drittland sitzt und dort seine Dienstleistungen oder Waren an Personen innerhalb der EU anbietet (und somit wieder personenbezogene Daten verarbeitet) ist man von der EU-DSGVO betroffen.

Ihr braucht also keine Auswanderung zu planen.

Weitere Info´s zur Frage, auf wen die DSGVO anwendbar ist, gibt es in unserer Info-Grafik:



So nun die wichtige und alles entscheidende Frage: **Was sind denn nun diese personenbezogenen Daten?**

Ihr fragt euch jetzt bestimmt heimlich „Vielleicht verarbeite ich ja keine und bin raus aus dem Schneider?“ Das ist oft die leise Hoffnung von einigen Mandanten - leider trifft es nie zu.

Personenbezogene Daten sind nach **Art. 4 Nr. 1 DSGVO** alle Informationen, die sich auf eine natürliche Person beziehen oder zumindest auf eine solche beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. – ÄH ja. Im Klartext heißt das:

Namen

Alter

Geburtsdatum

Anschrift

Lichtbild

E-Mail-Adresse

Telefonnummer

Kreditkartendaten

Bankverbindung

IP-Adressen

Neben diesen „normalen“ Daten gibt es auch noch die „besonderen Kategorien von personenbezogenen Daten“ – und diese genießen auch einen besonderen Schutz.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert.

Beispiele:

Lichtbilder auf denen die ethnische Herkunft zu sehen ist

Angaben zum Gesundheitszustand

Angabe von Allergien

Gut, wir wissen also nun, was personenbezogene Daten sind. Was ist denn nun dieses **Verarbeiten**?

Art. 4 Ziff. 2 DSGVO definiert die Verarbeitung von Daten wie folgt:

„Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“

Also bedeutet „Verarbeiten“ eigentlich alles 😊.

Ihr verarbeitet also z.B. personenbezogene Daten, wenn ihr

- Terminreservierungen telefonisch oder online anbietet
- Werbung an Kunden versendet
- Eine Kundenkartei führt (papier-basiert oder elektronisch)
- Testimonials für die Webseite nutzt

Ohne die Nutzung von personenbezogenen Daten würde euer Business also gar nicht funktionieren.

Auch Fotos von Kunden auf Social Media Plattformen oder der eigenen Website fallen unter die Verarbeitung personenbezogener Daten!

Jetzt geht es weiter mit dem wichtigsten Grundsatz, den ihr euch **UNBEDINGT** merken müsst.

### **Personenbezogene Daten dürfen nicht verarbeitet werden!**

Ich sehe die Fragezeichen in eurem Gesicht quasi vor mir. Aber es ist wichtig, dass ihr euch diesen Grundsatz einprägt. Denn er wird euch sensibilisieren, so dass ihr von alleine merken werdet, ob eine Verarbeitung von Daten in Ordnung ist oder eher nicht.

So. Also wir dürfen es grds. nicht – und jetzt kommt es: **außer** es liegen bestimmte Erlaubnistatbestände (ein wenig Juristendeutsch muss sein 😊)

Wir dürfen z.B. personenbezogene Daten verarbeiten, wenn wir sonst einen Vertrag nicht erfüllen können. Die Zusendung von Kosmetik z.B. wäre ohne Adresse schwierig ebenso wie die Terminabstimmung mit einer Kundin ohne deren Kontaktdaten zu nutzen).

Ebenso dürfen wir Daten verarbeiten und sogar die besonderen, wenn wir dafür eine wirksame Einwilligung eingeholt haben.

Wie eine solche Einwilligung aussehen muss schauen wir uns anhand des E-Mail Newsletters gleich genauer an.

Im Folgenden gehe ich auf einige für euch wichtige Beispiele genauer ein:

### Die Online-Reservierung

Die Kundendaten sind euer wichtigstes Gut.

Für die Anwendung der DSGVO macht es keinen Unterschied, ob Kundendaten handschriftlich oder elektronisch abgelegt werden. Das Gesetz sieht vor, dass die Speicherung der Daten zweckmäßig erfolgt. Das bedeutet, dass die Daten auch nur so lange gespeichert werden dürfen, bis der Zweck erfüllt ist. Und auch nur für den Zweck, für den du ursprünglich die Daten eingesammelt hast.

Im Klartext: Wenn mich jemand über das Kontaktformular auf meiner Seite anschreibt, darf ich ihn natürlich über die angegebene E-Mail-Adresse kontaktieren um diese Anfrage zu bearbeiten - ich darf ihm jedoch nicht einfach Werbung zusenden.

Denn das wäre ein anderer Zweck und für diesen habe ich KEINE Erlaubnis.

Genauso ist es bei Onlinereservierungen. Wenn der Termin stattgefunden hat müssten streng genommen die Daten anschließend gelöscht werden.

Damit man dieses nicht machen muss, sollte bei dem Termin eine Einwilligung eingeholt werden, um den Kunden in Zukunft auch telefonisch/ per E-Mail etc. ansprechen zu dürfen und zu diesem Zweck die Kontaktdaten weiterhin zu speichern.

Damit der Kunde aktiv seine Einwilligung erteilen kann, ist bei jeder Onlinereservierung eine Checkbox (so nennt man die Kästchen zum Ankreuzen oder Häkchen setzen) empfehlenswert.

Neben dem Link zu deinen Datenschutzbestimmungen, in welchen du definierst, wofür du die Daten speichern möchtest und für wie lange, sollte die Checkbox folgenden Wortlaut enthalten:

**Ich möchte, dass meine Daten auch nach Ablauf des Termins weiterhin gespeichert werden, damit ich zukünftig von NAME kontaktiert werden kann.**

## Der E-Mail Newsletter

Falls du nun noch die E-Mail-Adresse des Kunden für künftige Newsletter speichern möchtest, so muss auch dieser Vorgang explizit eingewilligt werden. In einer **weiteren Checkbox** muss der Kunden durch aktives Anklicken dem Erhalt von Newslettern ausdrücklich zustimmen.

### 1. Einwilligung

Denn eine Einwilligung muss nach der DSGVO folgende Merkmal erfüllen:

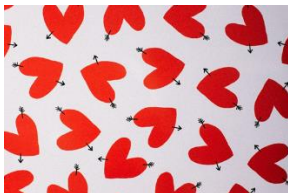
#### A. Freiwillig

Also ohne Zwang. Wir dürfen also nicht sagen: „Du kannst mein Produkt nur kaufen, wenn du dich auch in den Newsletter einträgst.“

Ebenso (wobei das heiß umstritten ist) sieht es mit unseren geliebten Freebies (so nennt man z.B. eBooks o.ä., die man kostenlos aber eben häufig gegen Anmeldung im Newsletter herunterladen kann) aus. Denn auch hier gibt es Ansichten, die sagen, dass die Leute gezwungen werden in den Newsletter zu kommen, um dann eine Leistung/ Produkt zu erhalten - obwohl diese Einwilligung für den Newsletter überhaupt nicht dafür erforderlich ist, dem Interessenten das Freebie zu geben.

Das heißt, wir verbinden 2 unterschiedliche Sachen fest miteinander („Koppeln“ diese = daher nennt sich das Ding auch Koppelungsverbot) die eigentlich unabhängig voneinander stehen.

#### No. 1 (Grüner Risikobereich)



Um es ganz klar zu sagen, die 100% Lösung sieht so aus, dass wir ein eBook, eine Checkliste o.ä. zur Verfügung stellen und die Landingpage so aufbauen, dass der Newsletter im Mittelpunkt steht und wir hier also Werbung für unseren Newsletter machen und erzählen was die Abonnenten alles Tolles erwartet.

**ABER** es gibt eine gesonderte Checkbox über die wir die Einwilligung für den Newsletter einholen. Die Checkliste bekomme ich auch so.

Jetzt denken sicher viele na toll: „Was soll das denn? Dann trägt sich ja niemand mehr in den Newsletter ein.“ Ist das so? Überlegt doch mal bitte, wann ihr das letzte Mal gezielt einen Newsletter abonniert hast. Ich weiß es noch für mich, das war bei Alexander Wiethaus von den E-Mail-Marketing Helden, denn ich möchte endlich lernen gute Sequenzen zu schreiben. Und was soll ich sagen, ich habe mich total auf den 1. Newsletter gefreut und diesen komplett gelesen und direkt weiterempfohlen – so wie hier. 😊.

Alle anderen Newsletter die sich so angesammelt haben, schaue ich ehrlich gesagt gar nicht mehr richtig an. Da war der erste Anreiz wirklich nur der Freebie und wenn der mich nicht überzeugt hatte, konnte es auch kein Newsletter hinterher. Und ich hätte auch sicher kein Produkt gekauft.

Daher bin ich persönlich davon überzeugt, dass sich eure Interessenten auch freiwillig in den Newsletter eintragen – gerade, weil ihr euer tolles Freebie (Content ist King) einfach so anbietet - und eben nicht die Leute ohne es zu sagen in einen Newsletter zieht.

---

Für alle, denen das aber zu „Blumig“ ist: Es gibt noch andere Ansichten zu dem Koppelungsverbot, die ich euch nicht vorenthalten möchte. Aber vorweg - KEINE dieser Varianten ist abmahnsicher – bis nicht ein Gericht darüber entschieden hat. Also Vorsicht und sicherheitshalber Rücklagen bilden! 😊

## **No. 2 (Oranger Risikobereich)**

Es gibt die Ansicht, die sagt: „Wir stellen einfach eine Wahlmöglichkeit her.“

Das heißt, man bietet auf einer Landingpage die Checkliste einmal gegen 9,99€ (Beispielspreis) und einmal gegen die Einwilligung, Werbe-E-Mails oder Anrufe zu bekommen, an. Hier ist wichtig, dass die Einwilligung ganz klar und so detailliert wie möglich beschrieben wird, damit der Interessent möglichst umfassend informiert wird was mit den Daten passiert; also wann und wie oft er zu welchen Themen von welchem Unternehmen angeschrieben wird.

## **No. 3 (Oranger Risikobereich)**

Wie No. 2, nur wir bieten die Checkliste nicht gegen Geld an, sondern tauschen Checkliste (Ware) gegen Daten (die wie Geld zu beurteilen sind). So entsteht nach dieser Ansicht ein Vertragsverhältnis - das könnte man durch AGB oder Nutzungsbedingungen noch ausgestalten und hat somit beides wirksam gekoppelt.

#### **No. 4 (Oranger Risikobereich)**

Wir verzichten auf eine Einwilligung und nehmen als Grundlage für die Verarbeitung der personenbezogenen Daten das sog. berechtigte Interesse nach Art. 6 Abs. 1 S.1 lit. f DSGVO. In dem dazu gehörigen Erwägungsgrund 47 wird das Direktmarketing als Beispiel für ein mögliches berechtigtes Interesse erwähnt. Ob darunter aber auch ein Newsletter fallen kann und wenn ja, unter welchen Voraussetzungen, kann man nicht mit absoluter Sicherheit sagen.

WICHTIG: Falls ihr diese Variante trotz des Risikos wählen möchtet, dann weist in der 1. E-Mail ausdrücklich auf das JEDERZEITIGE Widerrufsrecht hin. Das steht den Newsletter-Abonnenten immer auch ohne eine erklärte Einwilligung zu.

#### **No.5 (Roter Risikobereich)**

Alles bleibt wie es ist. Keine erweiterte Information und die Interessenten werden weiter in den Newsletter bei Freebie-Download gezogen.

### **B. Für den bestimmten Fall**

Eine pauschale Einwilligung in Form einer Blanko-Einwilligung ist unzulässig. Aus der Einwilligung muss erkennbar sein, welche personenbezogenen Daten zu welchem Zweck und von wem verarbeitet werden. Die Zwecke müssen möglichst genau bestimmt sein und dem Nutzer eine informierte Entscheidung ermöglichen.

Es ist erforderlich, klar anzugeben für welche Produkte oder Dienstleistungen man werben möchte bzw. um welche Themen es in dem Newsletter geht.

Soll der Newsletter an Bestandskunden nach § 7 Abs. 3 UWG geschickt werden, darf man auch die Formulierung „ähnliche“ wie von Ihnen erworbene Produkte/ Dienstleistungen verwenden.

### **C. Informiert**

Hier geht es darum anzugeben, wie oft der Newsletter erscheinen wird. Wenn ihr es nicht genau wisst, gebt sicherheitshalber eine häufigere Sequenz an.

### **D. Unmissverständlich**

Eine Opt-Out Möglichkeit ist nicht erlaubt. Der Interessent muss „tätig“ werden, durch aktives ankreuzen des Opt-Ins.

## PUH so die Einwilligung haben wir nun.

Kurze Pause ☺ – denn es geht natürlich noch ein wenig weiter.



## 2. Freiwillige weitere Angaben

Nach dem Grundsatz der Datenminimierung darfst du außer der E-Mail-Adresse KEINE weiteren Daten abfragen. Natürlich kannst du den Vornamen als optionales Feld mit anbieten, damit du später den Empfänger direkt bzw. personalisiert ansprechen kannst.

Werden freiwillig weitere Daten angegeben, sind diese von der Einwilligung des Betroffenen mitumfasst.

## 3. Jederzeitige Widerrufsmöglichkeit

Es muss dem Newsletter-Empfänger jederzeit möglich sein, seinen Widerruf der Einwilligung zu erklären. In jedem Newsletter muss darauf hingewiesen werden, dass diese Widerrufsmöglichkeit besteht und am besten wird auch direkt ein Link mitgesendet, über den dieser Widerruf möglich ist.

Jeder Widerruf muss dokumentiert und so verarbeitet werden, dass der Empfänger KEINE weitere E-Mail (mit Ausnahme der Abmeldebestätigung) mehr erhält.

Denn jede E-Mail nach einem Widerruf kann eine Abmahnung oder ein Bußgeld nach sich ziehen.

#### **4. Verweis auf die Datenschutzerklärung und das Impressum**

Dein Newsletter muss ein Impressum enthalten. Die Impressumspflicht im Newsletter ist im Telemediengesetz (TMG) in § 5 geregelt. Du musst deine Newsletter-Empfänger darüber aufklären, wer Absender des Newsletters ist (inkl. Anschrift). Hierfür kannst du den Footer im Newsletter verwenden. Dort sollte auch der Link zu deiner Datenschutzerklärung und zum Widerruf rein. Eine 3 in 1-Lösung sozusagen.

#### **5. KEINE Werbung in der Bestätigungs-E-Mail zum Double-Opt-IN**

Die Double-Opt-In E-Mails, also die Bestätigungsmails bei der Newsletter-Anmeldung, erhalten in der Regel sehr hohe Öffnungsraten und sind damit attraktiv für das Einbinden von Werbung. Dies ist allerdings nicht erlaubt, da der Nutzer zum Zeitpunkt zu dem er die E-Mail erhält, noch nicht dem Erhalt von Werbung zugestimmt hat. Das Unternehmenslogo darf jedoch in der E-Mail angezeigt werden.

#### **6. KEINE Werbung in der Abmeldebestätigung**

Hier gilt ebenfalls, dass auf Werbung komplett verzichtet werden muss.

#### **7. Nachweisbarkeit der Einwilligung**

Nach aktueller Rechtslage in Deutschland ist ein sogenanntes Double-Opt-In-Anmeldeverfahren (DOI) vorgesehen. Ein Empfänger bekommt bei der Anmeldung zum Newsletter eine Bestätigungsmail mit einem Bestätigungslink, bevor er aktiv in dem Newsletter-Verteiler aufgenommen wird. Erst wenn der Empfänger nun auch den Bestätigungslink in der Bestätigungsmail klickt, wird er aktiv in den Verteiler aufgenommen. Mit dem Double-Opt-In-Verfahren erfüllst du die Anforderung einer „ausdrücklichen Einwilligung“ bei der Newsletter-Anmeldung.

Die Einwilligung zum Newsletter solltest du in jedem Fall mit Text, Datum und Uhrzeit speichern, damit du diese im Ernstfall nachweisen kannst und die rechtliche Anforderung erfüllst.

#### **8. Datenschutzerklärung**

Damit sich deine Webseitenbesucher über die Verwendung ihrer personenbezogenen Daten rechtskonform informieren können, sollte deine Datenschutzerklärung einen Hinweis auf den Newsletter enthalten.

Hierbei solltest du beschreiben, was der Kunde von der Anmeldung zum Newsletter erwarten darf und was mit seinen Daten passiert.

Auch der Newsletter-Anbieter und die Rechtsgrundlage für die Datenverarbeitung (Das ist bei der Einwilligung Art. 6 Abs. 1 S. 1 lit. a) müssen genannt werden.

## **9. Auftragsverarbeitungsvertrag mit dem Newsletter-Anbieter**

Du gibst die personenbezogenen Daten an einen Dritten zum Newsletter-Versand weiter. Der Versanddienstleister sollte nach den Datenschutzkriterien ausgewählt werden (siehe Art. 28ff. DSGVO).

Nach Art. 28ff. DSGVO bist du dazu verpflichtet, vor der Weitergabe personenbezogener Daten einen sogenannten Vertrag zur Auftragsverarbeitung abzuschließen. Diesen Vertrag muss dir der Newsletter-Anbieter zur Verfügung stellen.

## **In 12 Schritten zum DS\_GVO konformen Newsletter 😊**

- ☐ Die Einwilligung erfolgt freiwillig (Stichwort Koppelungsverbot)
- ☐ Die Einwilligung ist für den bestimmten Fall formuliert
- ☐ Der Interessent wird umfassend informiert (Sequenzen, Unternehmen, Inhalte)
- ☐ Der Interessent versteht, dass er hier eine Einwilligung zu einem Newsletter abgibt
- ☐ Freiwillige weitere Angaben – nur E-Mail-Adresse ist verpflichtend!
- ☐ Jederzeitige Widerrufsmöglichkeit per Link in jeder E-Mail
- ☐ Impressum in jeder E-Mail und Verlinkung auf die Datenschutzerklärung
- ☐ KEINE Werbung in der Bestätigungs-E-Mail zum Double-Opt-IN
- ☐ KEINE Werbung in der Abmeldebestätigung
- ☐ Double-Opt-In
- ☐ Aktuelle Datenschutzerklärung mit Passus E-Mail Newsletter
- ☐ Auftragsverarbeitungsvertrag vom E-Mail Newsletter Anbieter

### DISCLAIMER

Dieses Dokument dient einer allgemeinen Information und stellt KEINE Rechtsberatung im Einzelfall dar. Sämtliche Muster müssen auf den Einzelfall angepasst werden. Zudem wird keine Gewähr für Aktualität und Vollständigkeit übernommen. Die Vervielfältigung ist kostenlos unter Verwendung der Urheberkennzeichnung gestattet.

### **Bestandskunden sind doch etwas Schönes:**

Nach Art. 7 Abs. 3 UWG, Art. 16 Abs. 2 ePrivacy-VO-E ist es – wenn die Voraussetzungen dieser Norm vorliegen zulässig OHNE Einwilligung E-Mails zu versenden! YEAH, endlich mal eine gute Nachricht !!!

Auch ein Opt-Out ist hier ausnahmsweise gestattet, da man von einem berechtigten Interesse, dass wir als Unternehmer an Direktwerbung haben, ausgeht (Art. 6 Abs. 1, S.1 lit. f). Das bedeutet, hier darf das Kästchen vor-angekreuzt sein.

Zudem rechne ein Bestandskunde damit, dass er Werbung zu ähnlichen wie den gekauften Produkten erhalte. Der Kunde sollte darüber aber in Kenntnis gesetzt werden und auch ohne erteilte Einwilligung auf sein jederzeitiges Widerrufsrecht hingewiesen werden.

### **In 8 Schritten zum DS-GVO konformen Newsletter bei Bestandskunden ☺**

- ☐ Bestandskunde nach § 7 Abs. 3 UWG. (Dann ist eine Einwilligung entbehrlich)
- ☐ Einwilligung ist auch mit Opt-Out bei der Bestellung möglich- aber klar kennzeichnen!
- ☐ Widerrufsmöglichkeit in 1. Email bei Bestandskunden eingerichtet
- ☐ Inhalt Newsletter für Bestandskunden nur für ähnliche Produkte
- ☐ Verweis auf die Datenschutzerklärung und das Impressum in jeder E-Mail
- ☐ KEINE Werbung in der Abmeldebestätigung
- ☐ Aktuelle Datenschutzerklärung mit Passus E-Mail Newsletter
- ☐ Auftragsverarbeitungsvertrag vom E-Mail Newsletter Anbieter

### **Gewinnspiele und Werbeeinwilligungen:**

Gewinnspiele und Werbeeinwilligungen gegenüber Drittunternehmen sind ja auch sehr beliebt. Bitte zukünftig darauf achten, dass es natürlich möglich ist, eine Einwilligung für den Werbeversand auch für ein Drittunternehmen- welches natürlich benannt werden muss- einzuholen. Allerdings darf die Teilnahme am Gewinnspiel nicht an die Einwilligung in den Erhalt von Werbung geknüpft werden.

Genau – das Koppelungsverbot schlägt wieder zu. Auch hier gelten die oben angegebenen Hinweise und Möglichkeiten.

### **Auftragsdatenverarbeitung nach der DSGVO**

Der Versand von Newslettern, die externe Lohn- und Gehaltsabrechnung, die externe Rechnungsbearbeitung / Buchhaltung, Papier- und Aktenvernichtung sowie die Vernichtung von Datenträgern durch externe Dienstleister sind Datenverarbeitungsvorgänge, die dem Datenschutzrecht unterliegen. Es ist eine sogenannte **Verarbeitung von Daten im Auftrag** und diese erfordert einen Vertrag. Sie muss den Anforderungen von Art. 28 DSGVO entsprechen. Außerdem müssen technische und organisatorische Maßnahmen nach Art. 32 DSGVO ergriffen werden, um den Schutz der Daten gewährleisten zu können.

Auch die Frage, wo der externe Dienstleister seinen **Sitz** hat, muss geklärt werden. Es macht datenschutzrechtlich einen Unterschied, ob die Datenverarbeitung bei den Anbietern und Dienstleistern außerhalb der EU (Drittstaat) oder im Geltungsbereich der EU-Datenschutzgrundverordnung erfolgt. Insbesondere gilt dies für die Datenverarbeitung in den USA oder durch US-Unternehmen. Die Verarbeitung in Drittstaaten ist nur rechtmäßig, wenn die Grundsätze der Datenverarbeitung in Drittstaaten berücksichtigt werden (Art. 44 DSGVO).

Von der Datenverarbeitung in Drittstaaten sind insbesondere Anbieter für den Newsletter-Versand betroffen.

## Speichern und Löschen von Daten nach DSGVO

Personenbezogene Daten dürfen grundsätzlich nur solange verarbeitet werden, wie dies zur Erfüllung des Zweckes, zu dem sie erhoben wurden, notwendig ist. Sie sind anschließend zu löschen und dürfen somit nicht dauerhaft gespeichert werden.

Wenn ihr Produkte verkauft, solltet ihr die Daten in jedem Fall 24 Monate aufheben, da immer noch Gewährleistungsansprüche durch den Kunden geltend gemacht werden könnten.

Zudem müsst ihr natürlich die steuerrechtlichen Aufbewahrungspflichten beachten - selbst wenn ein Kunde von euch verlangt alle Daten zu löschen - gehen diese gesetzlichen Fristen vor. Wenn ihr dann die Daten nicht mehr braucht, müsst ihr diese natürlich komplett löschen.

Wo die Daten gesichert werden, in welchem Land der Server steht, ob die Kundenkartei sicher aufbewahrt wird oder die Frage danach, wer Zugriff auf die Daten hat muss geklärt und eigenverantwortlich dokumentiert werden, um für die Sicherheit der Daten zu sorgen. Falls dies kontrolliert wird, musst du all jene Informationen darlegen können. Es gilt, dass nur die Mitarbeiter, die zur Vertragserfüllung, also für den Termin mit dem Kunden bestimmte Informationen (z.B. Allergien) benötigen, Zugriff auf diese Daten bekommen. Nicht jeder Mitarbeiter sollte Zugriff auf alle Daten jedes Kunden haben können und es sollte in jedem Fall eine Verschwiegenheitsvereinbarung getroffen werden.

Wenn ihr bis hierhin durchgehalten habt, dann habt ihr euch die Blumen redlich verdient. Jetzt folgt eine Checkliste, sodass ihr direkt loslegen könnt. Ich bin jetzt schon wirklich stolz auf euch, denn nach einer aktuellen Umfrage ist noch nicht mal jedes 3. Unternehmen dabei, sich gerade mit der DSGVO zu befassen - ihr gehört also zu den Mutigen die den Schritt gemacht haben!



### DISCLAIMER

Dieses Dokument dient einer allgemeinen Information und stellt KEINE Rechtsberatung im Einzelfall dar. Sämtliche Muster müssen auf den Einzelfall angepasst werden. Zudem wird keine Gewähr für Aktualität und Vollständigkeit übernommen. Die Vervielfältigung ist kostenlos unter Verwendung der Urheberkennzeichnung gestattet.

Geht die Punkte Schritt für Schritt durch und wenn Fragen aufkommen:

Mich findet ihr hier: [www.lawlikes.de](http://www.lawlikes.de)

## Checkliste

### ☐ **Bestandsaufnahme**

Verschaffe dir einen Überblick, wo du überall personenbezogene Daten verarbeitest – denk daran verarbeiten bedeutet nicht nur AKTIV Daten irgendwo einzupflegen, sondern auch wenn automatisch- wie z.B. bei Google Analytics- Daten verarbeitet bzw. weitergegeben werden.

Stell dir dazu vor, du hättest Interesse an deiner eigenen Dienstleistung – wie wird man dein Kunde? Was machst du, wenn man Kunde ist - welche Daten benötigst du dann und wie kommen die Daten zu dir? Der Weg der Daten ist also wichtig!

### ☐ **Webseite**

Ist deine Webseite bereits SSL verschlüsselt?

Ist dein Online-Buchungstool ebenfalls verschlüsselt?

Ist dein Kontaktformular verschlüsselt

Hast du eine individuelle Datenschutzerklärung, die alle Cookies und Plug-Ins auf deiner Webseite berücksichtigt? Um herauszufinden, was du alles auf der Webseite einsetzt, solltest du deinen Webdesigner fragen!

Hast du ein vollständiges Impressum?

### ☐ **Auftragsverarbeiter und die Verträge dazu**

Hast du Auftragsverarbeitungsverträge mit deinem Webseiten-Hoster, mit deinem Buchungstoolanbieter, mit deinem Newsletter Anbieter, mit deiner virtuellen Assistentin, mit Google-Analytics u.s.w.?

### ☐ **Newsletter**

Dein Newsletter ist optimal eingerichtet?! (Vorgaben siehe oben)

### ☐ **Einwilligung**

Hast du ein Einwilligungsformular, dass es dir erlaubt, deine Kunden rechtssicher anzusprechen – das Formular muss sehr detailliert sein und mehrere Einwilligungen enthalten. Z.B. einmal, um Kontakt per Whats-App aufzunehmen, einmal gesondert, um Bilder als Testimonial zu verwenden.

☐ **Formulare**

Überprüfe die bislang verwendeten Formulare (z.B. Aufklärungs- und Einwilligungsbögen sowie Zustimmungserklärungen in AGB und auf deinen Webseiten). Achte vor allem darauf, dass du nur die notwendigen Daten abfragst. Wenn du Gesundheitsdaten (Allergien etc.) abfragst, lass dir die Verwendung dieser besonderen personenbezogenen Daten durch eine Einwilligung genehmigen.

☐ **Datenlöschung**

Wenn du die Kundendaten nicht mehr benötigst, solltest du diese löschen. Du solltest, wenn ein Kunde ein Produkt gekauft hat, die Daten auch zum Kauf für 24 Monate aufheben. Denn solange könnte er noch einen Gewährleistungsanspruch geltend machen. Die Rechnungen und alles was du für die Buchhaltung benötigst, musst du 10 Jahre aufbewahren.

---

So, das war's fürs Erste. Mehr von uns findest du hier: [www.lawlikes.de](http://www.lawlikes.de)

Viele Grüße

Deine Sabrina Keese-Haufs